Cybersecurity Foundations

Introduction to Cybersecurity & Digital Protection

Target Audience

High School Students (Grades 9–12) and beginners who want to develop a strong foundation in computers, networking, cybersecurity concepts, digital safety, and basic security practices. No prior cybersecurity experience is required.

Program Pathway

Cybersecurity Foundations

Total Duration

72 Hours

Delivery

Cohort-Based + Instructor-Led + Hands-On Labs

Program Goal

The Cybersecurity Foundations program introduces students to the fundamentals of cybersecurity, computer systems, networking, programming concepts, cyber threats, security controls, and digital protection. Students develop foundational technical and security skills through instructor-led lessons, practical activities, guided labs, cybersecurity scenarios, assessments, and a final Cyber Safety Capstone.

The program is designed to establish the knowledge required to progress into the **Cybersecurity Practitioner** pathway.

Program Structure

Module	Topic	Hours

Module 1	Digital World & Cybersecurity Fundamentals	14
Module 2	Computer Systems & Operating Systems	16
Module 3	Networking Fundamentals	16
Module 4	Programming Foundations for Cybersecurity	14
Module 5	Cyber Safety Capstone & Security Fundamentals	12
Total		**72 Hours**

Curriculum

Module 1 – Digital World & Cybersecurity Fundamentals

Students are introduced to the digital world and develop an understanding of cybersecurity, common cyber threats, security principles, and responsible digital behavior.

Topics:

Digital World Fundamentals, Introduction to Cybersecurity, Importance of Cybersecurity, Cybersecurity Domains, Information Security Fundamentals, Confidentiality, Integrity & Availability, Authentication & Authorization, Digital Identity, Password Security, Multi-Factor Authentication, Social Engineering, Phishing, Malware Fundamentals, Viruses & Worms, Trojans, Ransomware, Spyware, Common Cyber Attacks, Cybersecurity Threat Actors, Insider Threats, Cybersecurity Risk Fundamentals, Personal Data Protection, Privacy Fundamentals, Safe Internet Practices, Cyber Ethics, Responsible Digital Behavior.

Module 2 – Computer Systems & Operating Systems

Students learn how computers work internally and how operating systems manage users, applications, files, processes, memory, and system resources.

Topics:

Computer Hardware Fundamentals, CPU, Memory & Storage, Input & Output Devices, System Components, Software Fundamentals, Operating Systems, Windows Fundamentals, Linux Fundamentals, macOS Fundamentals, Files & Directories, File Permissions, Users & Groups, Processes, Services, Applications, System Resources, System Configuration, Software Updates, Security Updates, Antivirus & Endpoint Protection, Firewalls, Secure System Configuration, User Account Security, Access Control Fundamentals, System Logs, Backup Fundamentals, Data Protection, Secure Computing Practices.

Module 3 – Networking Fundamentals

Students develop a practical understanding of how computers communicate across networks and how networking technologies support cybersecurity.

Topics:

Networking Fundamentals, Network Types, LAN, WAN & Internet, Network Devices, Switches, Routers, Wireless Access Points, Network Topologies, OSI Model Fundamentals, TCP/IP Model, IP Addresses, IPv4 Fundamentals, IPv6 Introduction, MAC Addresses, Ports & Protocols, TCP & UDP, DNS, DHCP, HTTP & HTTPS, SSH, FTP & SFTP, Network Address Translation, Subnetting Fundamentals, Default Gateway, Routing Fundamentals, Wireless Networking, Wi-Fi Security, Network Security Fundamentals, Firewalls, Network Segmentation, VPN Fundamentals, Network Monitoring Fundamentals..

Module 4 – Programming Foundations for Cybersecurity

Students develop basic programming and scripting skills that can be applied to cybersecurity tasks, automation, data processing, and security analysis.

Topics:

Introduction to Programming, Programming Logic, Algorithms, Variables, Data Types, Operators, Conditional Statements, Loops, Functions, Lists & Dictionaries, Strings, User Input, File Handling, Error Handling, Basic Python Programming, Python for Cybersecurity, Data Processing, Text Processing, Pattern Matching Fundamentals, Regular Expressions

Introduction, Basic Automation, Working with Logs, Security Data Analysis, Simple Security Scripts, Ethical Programming Practices.

Module 5 – Cyber Safety Capstone & Security Fundamentals

Students apply the concepts learned throughout the program to identify cybersecurity risks, analyze security scenarios, implement basic protections, and demonstrate foundational cybersecurity skills.

Topics:

Cybersecurity Risk Identification, Threat Identification, Vulnerability Fundamentals, Security Controls, Authentication & Access Control, Endpoint Security, Network Security Fundamentals, Data Protection, Password & Identity Security, Phishing Awareness, Social Engineering Awareness, Security Policies, Incident Identification, Incident Response Fundamentals, Security Monitoring Fundamentals, Backup & Recovery, Cybersecurity Best Practices, Security Documentation, Security Awareness, Cyber Ethics, Capstone Planning, Security Assessment, Final Presentation.

Hands-On Learning

Students learn through instructor-led lessons, cybersecurity demonstrations, computer-system activities, networking exercises, Python programming activities, security scenarios, guided labs, threat-analysis exercises, assessments, mini-projects, and a final Cyber Safety Capstone project.

Students are gradually introduced to cybersecurity concepts rather than being expected to have prior technical knowledge.

What Students Build

Students develop practical experience with:

- Cybersecurity fundamentals
- Digital security and privacy
- Password and identity protection
- Phishing and social-engineering awareness
- Computer systems and operating systems
- Windows and Linux fundamentals
- Files, permissions and users
- System processes and logs
- Networking fundamentals
- IP addressing and subnetting
- Network protocols
- DNS and DHCP
- Network troubleshooting
- Basic network security
- Python programming
- Security scripting
- Log analysis
- Basic security automation
- Cybersecurity risk assessment
- Security controls
- Incident-response fundamentals
- Cyber safety planning
- Final cybersecurity assessment

Recommended Lab Requirements

Each student should ideally have:

- Windows or Mac desktop/laptop
- 8 GB RAM minimum
- 16 GB RAM recommended
- 10 GB+ free storage

Windows or Mac systems are recommended.

Students may use Linux through a virtual machine or cloud-based environment for selected cybersecurity labs.

A dedicated GPU is **not required** for this program.

Virtual machines and cloud-based environments may be used for selected Linux, networking, programming, and cybersecurity exercises.

Next Step

Students who complete **Cybersecurity Foundations** will have a strong understanding of computers, operating systems, networking, programming fundamentals, cyber threats, security controls, and digital protection.

Students can progress to the next pathway:

Cybersecurity Practitioner

The next level can introduce students to more advanced areas such as network security, vulnerability assessment, ethical hacking fundamentals, security monitoring, incident response, cloud security, identity and access management, and security operations.